What is claimed is:

1. A system for preventing illegal use of software, comprising:

secret information storage means for storing secret information;

cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means;

illegal access determining means for determining whether an illegal access to the system is performed; and

cryptosystem key updating means for:

providing the same key for a cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if the illegal access determining means detects no illegal access;

providing different keys for the above two kinds of cryptosystem keys if the illegal access determining means detects an illegal access; and

wherein the cryptosystem key updating means updates the above two kinds of cryptosystem keys for each access to the system.

2. A method for preventing illegal use of software, the method used in a system which comprises a secret information storage means for storing secret information and a cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means, the method comprising the steps of:

determining whether an illegal access to the system is performed; and

for each access to the system,

providing the same updated key for a cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if no illegal access is detected in the step of determining whether an illegal access to the system is performed;

providing different updated keys for the above two kinds of cryptosystem keys if an illegal access is detected in the step of determining whether an illegal access to the system is performed.

3. A storage medium storing a computer-executable program for preventing illegal use of software, the program used in a system which comprises a secret information storage means for storing secret information and a cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means, the program including the processes of:

determining whether an illegal access to the system is performed; and

for each access to the system,

providing the same updated key for a cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if no illegal access is detected in the step of determining whether an illegal access to the system is performed;

providing different updated keys for the above two kinds of cryptosystem keys if an illegal access is detected in the step of determining whether an illegal access to the system is performed.

4. A system for preventing illegal use of software as claimed in claim 1, wherein the secret information storage means and the cryptosystem key storage means are separately constructed.

5. A method for preventing illegal use of software as claimed in claim 2, wherein the secret information storage means and the cryptosystem key storage means are separately constructed.

6. A storage medium storing a computer-executable program for preventing illegal use of software as claimed in claim 3, wherein the secret information storage means and the cryptosystem key storage means are separately constructed.

7. A system for preventing illegal use of software as claimed in claim 1, wherein the system is applied to an IC card.

8. A method for preventing illegal use of software as claimed in claim 2, wherein the system in which the method is used is applied to an IC card.

9. A storage medium storing a computer-executable program for preventing illegal use of software as claimed in claim 3, wherein the system in which the program is used is applied to an IC card..